IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

TITLE:

INTERNET CONNECTION USER COMMUNICATIONS SYSTEM

INVENTORS:

Donzis; Henry M. (San Antonio, TX)

Donzis; Lewis T. (San Antonio, TX)

Frey; Rodney D. (San Antonio, TX)

Murphy; John A. (San Antonio, TX)

Schmidt; Jonathan E. (San Antonio, TX)

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of Application U.S. Serial No. 10/023,674, entitled: "INTERNET PROVIDER SUBSCRIBER COMMUNICATIONS SYSTEM", filed on December 18, 2001. Priority is claimed.

BACKGROUND OF THE INVENTION

Field of the Invention

[01] The invention is generally related to customer relations and management communication systems and is more specifically directed to a method for the enforced delivery of messages to customer subscribers and users of an Internet Service or transport service provider.

Discussion of the Prior Art

[02] Over the next several years in the U.S., 85 million new users will start using the Internet and 77% of U.S. households will be connected to the Web. Clearly, the Internet market will continue to grow in existing and altogether new ways. The Internet is now a critical part of our communications options. Innovation will continue to be a major factor associated with the Internet as enterprising companies find new ways to offer faster, more expanded services ranging from access, security, quality and class of services, as well as content offerings. No matter what these expanded services or applications turn out to be, the rapid adoption of Internet use will continue to increase and that increase will have profound effects on the providers who support these millions of users.

[03] Currently, the providers that physically connect subscribers to the Internet are very limited in their ability to communicate back to their subscriber base. If a provider wants to communicate with customers about planned outages or problems, viruses being broadcast from the subscriber PCs, billing issues, or emergency information, the provider is limited to some very unreliable approaches such as phone calls, e-mails, or bulletins in monthly billing statements. None of these approaches offer assured timely delivery, and most require a great deal of effort with uncertain results. Today, the common method used to notify the subscriber is to let the subscriber discover the particular problem and then contact the provider for assistance and information. Unlike cable television wherein the cable company can force "crawlers" and other informational communication to the viewer's television screen, the Internet service provider must rely upon the subscriber to voluntarily and manually access the informational Web pages that relate to the subscriber's system. The subscribers of the provider may not use or reveal other services that might have been useful such as their use of e-mail or even their e-mail addresses. The other customer relations communication channel used by the provider is the accompanying flier that is mailed with the monthly bill. These channels are unreliable and not timely for much of the communication that the provider could utilize that would substantially reduce the cost of supporting the subscriber base. A simple example is enforced notification of scheduled system "down time" due to maintenance. Virtually all subscribers who are notified of an upcoming service interruption will not place the support telephone calls that typically inundate the provider support facilities under such circumstances.

[04] Due to the ever growing Internet user population, a solution that could avoid these calls would not only greatly reduce the unnecessary call volume being placed on provider call support

centers, but would also help improve customer confidence, leading to better customer loyalty and retention.

[05] Enforced delivery of messages has been available with auxiliary client software components such as enrollment and use of an "Instant Messaging" system as offered by AOL and Microsoft. Enforced delivery of messages has also been available with auxiliary client software components associated with certain provider authentication protocols. In all cases, the software becomes machine, operating system, and operating system version dependent, must be installed by the subscriber or user, and the installation must be supported by the provider.

[06] U. S Patent No. 6,148,332, entitled: MANDATORY **MESSAGE DISPLAY AND REPORTING SYSTEM**, issued to C. M. Brewer on November 14, 2000 discloses a messaging system including a software program to be loaded on a PC that is closely linked to the PPP ("The Point-to-Point Protocol," as defined by RFC 1661) or PPPoE ("A Method for Transmitting PPP Over Ethernet," as defined by RFC 2516) that the Internet service provider provides. Specifically, this is "LOG-ON" software that the user must have in order to initiate and maintain service. The intent of the application is to force advertising windows on the user's screen, i.e., a mandatory display. The main components of this system are that the software must be loaded on the user PC, the window is specifically not on the Web browser, and the advertising window cannot be removed without losing the connection to the Internet service provider service.

[07] In addition to ISP support systems, it is becoming increasingly desirable to support inter-communication between a user and a local, sub-level provider, such as an establishment or transportation provider supplying Wi-Fi connectivity for its customers or passengers. The Wi-Fi "hotspot" market is anticipated to grow to a half-million within four years. Hotspot providers

have no access to their own provision channel in order to push advertisements to their users other than at sign-on time...that is, once per visit. The overriding problem in this phenomenon is the conflict between the exploding popularity and the lack of a way to make manage it from a cost/risk aspect. Currently, there are three ways that providers attempt to gain value from the installation of a hotspot:

- Charge for the service as you use it (not popular with users) but may work for critical areas like airline clubs, captive passengers in a train or airplane, and other public access areas, where users who really need it will pay for it.

- Associate a free use of the service with other products such as a DSL or cable modem home subscription.

- Use the service as a way to attract customers to your store such as anticipated by chain restaurants and the like.

SUMMARY OF THE INVENTION

[08] The subject invention specifically eliminates a requirement for any client software components and specifically utilizes Web page access. Automatic modification of the content of received data also can be accomplished with other unmodified Web applications in accordance with the invention. The invention presents a Web page as a replacement for the user-requested page, as an interim page before the requested page, or as an additional "pop-up" browser window. Enforcement takes advantage of the near-universality of Web browser utilization and of the protocol to log successful deliveries. In accordance with the teachings of the invention, the elimination of a client software component can create the entirety of the functionality of the

system in a hardware or software device that can be distributed throughout the provider infrastructure through a simply installed, fail-safe network connection without customer participation in the installation process.

[09] The architect of the invention is adopted to unobtrusively co-exist with the current Internet transport networks, providing critical performance monitoring and automated messaging to insure that transport network operators, ISPs, content providers, and the users have communication links. This can include aggregation routers of typical ISPs, neighborhood connectivity at the ISP CMTS level and even hot-spots such as Wi-Fi connections at a retail establishment level.

[10] The method of the subject invention provides users with active screens informing them of transport or Internet Service Provider network problems, thus allowing customers to know of any situation real-time and avoid overwhelming the provider's congested call-centers with costly and unnecessary trouble-report calls. In addition, users will be able to monitor their own Internet performance and differentiate problems between transport and content parties and avoid the costly inquiry calls that would otherwise occur. The estimated payback in technical support call reduction alone is a matter of a couple of months with indirect customer satisfaction increasing the true value much more. The reduction of technical support center calls provides a very attractive payback to the providers. In addition, other services may be offered by facilitating localized content delivery such as emergency information and/or advertising. Once the invention, which may be implemented as a hardware device, or as software running on a standard computer system, is merged within the provider network, additional services are provided through software upgrades at the provider without requiring installation at the user's site. Specifically, all of this is done within the network without touching user equipment.

[11] The subject invention allows providers to have an active vehicle with which to communicate to a user (or subscriber group) while the user is browsing the Internet. These services are manifested in a number of ways depending on the providers' physical and logical network architecture. The methodology is addressable to all IP provider connection approaches from Broadband (Cable, DSL, Satellite, Fixed Wireless) to traditional dial-up services.

[12] In addition to offering the provider a cost savings proposition in technical support call elimination and in improving customer confidence, the system of the subject invention also offers the Provider a way to directly reach users by particular demographics for emergency information and advertising purposes. Within the realm of advertising, the ability to tie ad content to local geographics, as well as user demographics, will allow very specific ad content to be presented to users. Such high quality advertising can result in incremental provider revenue as well as open up the opportunity for expanded products that provide Internet access at a lower price because of advertising subsidization.

[13] The preferred embodiment of the invention can be entirely contained within a hardware or software device that is connected to the provider network that performs the modification of the Web information delivered to the user. The enforcement can be guaranteed with Web browser activity by the targeted user. The near-universality of Web browser utilization by Internet users presents a near-universal enforcement of the desired customer management communication from the provider to the user and on a real-time basis and confirmation of delivery is available both from system logs as well as optional Web page click-through.

[14] The provider creates the special communication through the three-part definition:

1. the resolution from IP address to a customer identification by account number, modem MAC address or serial number, other fixed identifier, or temporary identifier such as cookie placement to meter the delivery frequency.

2. The policy of delivery describing the circumstances of delivery such as time of delivery, frequency, triggering activity, and the like.

3. The associated Web page or other content to be delivered and type of page delivery (replacement, insert, pop-up).

[15] The system relies upon any of several standard router mechanisms to redirect Web traffic. Some existing protocols developed for transparent Web caching permit the installation to take place while the system is fully operational and renders it immune to device failure by supporting normal functionality should the device fail. These protocols are preferred but not necessary.

[16] The system examines the source IP address of a request and, if not cached, makes a query to obtain the customer identification to check if a policy is in force. There are different protocol options that can be utilized to obtain this relationship that may be kept in DNS (Domain Name System), DHCP ("Dynamic Host Configuration Protocol," as described in RFC 1531), LDAP ("Lightweight Directory Access Protocol," as described in RFC 1777), or external database servers. The device endeavors to utilize the valid duration of these relationships to cache the information and reduce network administrative message overhead.

[17] When policies are not necessarily directed at specific users but, instead, to IP address-identified individuals or subnets, the delivery process can proceed without user-lookup but with metering based upon the IP address alone. The use of cookies placement and cookie examination by visible or non-visible, null-Web pages can control the metering of the delivery to groups of users. The cookie-based metering can, additionally, include effective metering control of users who experience IP address changes during the delivery schedule and to individual users in a group of multiple users behind address-translating routers exhibiting a single IP address to the Internet.

[18] When no policy is in force for a particular user or group of subscribers, the connection is allowed to proceed normally and the expected Web page is displayed. If a policy is in force for that user, the policy is enforced and, as an example, the user may see a "pop-up" browser window appear containing special customer communications. The pop-up window can request further action or utilize any of the rich array of options available in Web browsers.

[19] In systems with many devices connected, an optional management console can be utilized to consolidate the numerous devices into presenting itself as a single system to the existing provider infrastructure. This consolidation can reduce or eliminate administrative overhead of the existing provider infrastructure when expanding or changing the system of devices. The management console can also consolidate the administrative activity of the Web redirecting devices to reduce that overhead.

[20] In addition, systems that utilize alternative address management databases to reconcile subscriber account identification with currently issued IP addresses can be used identically to the DHCP query for Cable Modem address within the consolidating and management device by

substituting the alternate account identification for the Cable Modem address or unique subscriber ID and subsequently relaying the respective policy information for that subscriber to the redirecting device upon discovery of the associated IP address.

[21] Alternatively, the redirecting device reflects packets back to the router while maintaining state information about the browsing session. Once an HTTP GET message is seen and the URL and HTTL header are examined, if it is desired to send a replacement message, the redirecting device replies directly to the user, as if it is the server, and the redirecting device sends a message to the server, as if it is the client, that terminates the session. If the page is not to be replaced, the redirecting device can simply continue to reflect packets back to the router.

[22] In a further implementation of the system, the Cable MSO is replaced with a hotspot network. Both are Internet providers with the difference being one of scale, with the latter being much more appropriately associated with the advertising application as opposed to the service/support application. In a typical application of this configuration, the hotspot infrastructure appears in two basic classes:

a) Hotspots independently connected directly to the Internet through a firewall using a NAT (many-to-one address translation) whereas all traffic from users to the Internet hops onto the Internet at the site; and

b) Hotspots VPN'd in one way or another such that all users are given addresses of a core provider's remote network and "tunneled" back to a central network for control.

[23] The centrally owned instance that also tunnels all users back to a central network can be serviced very much like that of a cable Internet provider.

[24] The small, directly-connected, independently installed, opportunistic provider can be serviced by a two-terminal device that would install in the cable between the Internet service and the hotspot NAT router and transmitter/receiver called an Access Point (AP). Such a system requires little or no access to identifying the actual user either to target advertising as appropriate or to meter the frequency of pop-up ads to individuals at the ISP level, while such an application is supported at the user level, permitting the provider to communicate with each user on a one-to-one basis. Specifically, the identification of the users, who are anonymous to the Internet traffic because they are on the other side of the NAT, is supported by the subject invention. Users behind such a NAT can receive evenly dispatched messages that can be metered through the use of the placement and examination of cookies by the Web interaction with the device through either visible or non-visible null Web pages that process the cookie tagging.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the two components of the invention: the redirecting device and the consolidating and management device.

Figure 2 shows the redirecting device at the network edge with the cable access concentrator/router and other various network components.

Figure 3 provides a summary of how the redirecting device navigates through the four critical modules.

Figure 4 shows alternate locations on a network incorporating the redirecting device of the subject invention.

Figure 5 shows the redirecting device as utilized on a Wi-Fi system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[25] The architecture of the preferred invention is designed especially to adapt to a cable operator's IP network. Comparable components and protocols exist in other broadband systems such as DSL and wireless, as well as other Internet service provider transports, such as analog and digital dial-up and private line environments, for which the scope of the invention is intended to include.

[26] Internet service and transport providers provide their users with a pipeline to the Internet, but are not directly involved in the content obtained by those users. Typically, this pipeline is transparent to the user, with no modification of its content along the path. In some cases, web caching or other performance enhancement technology may be provided, but this still strives to maintain the original content. The invention provides a method and apparatus whereby this content may be modified or replaced along the path to the user. For the purposes of establishing a reliable delivery of bulletin messages from providers to their users, the invention specifically forces the delivery of specially-composed World Wide Web browser pages to the user, although it is not limited to that type of data. These may be displayed permanently, temporarily, or in separate pop-up browser windows, according to policies set by the provider irrespective of the user's intended browsing destination. The result of this system is the ability of the provider to make use of communications to users without the requirement of a special client software component to be present on the user's personal computer or other browsing device. Another benefit of the invention is its implementation as a hardware or software device that incorporates simplified, fail-safe integration into the provider's infrastructure. In addition, due to the use of the standards of World Wide Web browsers, all the Web features, such as interactivity in the

same or separate pop-up windows, become available to the provider. The policies set by the provider can be for specific users or groups of users with identified characteristics or activity.

[27] Over 90% of cable television system operators in the United States provide high speed (broadband) Internet access through their system with an early adoption rate of 8% in the U.S. and 5% globally.

[28] Cable systems, upgraded to serve digital channels, can support data-over-cable Internet access through the industry standard, DOCSIS, which sends the Internet data inside a compatible packet in the same form as digital TV's MPEG2. In addition to supporting MPEG2 digital television, the Internet access infrastructure is required to support upstream data in the 5 to 45MHz spectrum for the 2-way Internet activity.

[29] A variety of early adopters experimented with several schemes to transport two-way data over existing cable infrastructure, however, DOCSIS emerged as the standard. The DOCSIS 1.0, 1.1, and 2.0 Radio Frequency Interface (RFI) Specification SP-RFI-I05-991105 is what the majority of US vendors and cable operators have agreed to implement. In addition, the industry supports an interoperability laboratory that tests and enforces compatibility complete with certification labels.

[30] The spectrum on the cable plant allows for downstream, or forward, path signals that occupy the 54- to 860-MHz band, with channels spaced at the standard 6 MHz originally designed to handle the over-the-air: NTSC video signals. In fact, the entire cable infrastructure retains this channelized imprint from the over-the-air spectrum.

[31] The upstream, or return path DOCSIS signals generally occupy from 5 to 42 MHz (a spectrum not used by over-the-air television and, in fact, is the spectrum used by "short wave" broadcast when propagated over the air). The upstream spectra can, therefore, have variable channel spacing, depending on the signal's type and format. Because of the noisy and legacy design implications, upstream signals with DOCSIS are limited in bandwidth and, as with the Cisco CMTS (Cable Modem Termination System), broken up into six upstream segments each individually allocated to a small neighborhood of approximately 200-300 houses.

[32] The choice of employing compatibility with the legacy 6MHz channelization permits compatibility with other parts of the system allowing a minimal amount of disruption to the existing infrastructure when it DOCSIS-compatible Internet data access is added. In addition, much of the upgrades in plant and equipment required for the provisioning of broadband Internet access are in common with the upgrades needed to expand service to digital television services and pay-TV which can fit from 4 to 12, typically 6, digital channels into each of the same 6MHz channels of the spectrum.

[33] The digital channels have digital data encoded in MPEG2 frames that include the DOCSIS data. The DOCSIS data can utilize an entire 6MHz channel or be interleaved with other services but that is not known to be a feature that is utilized. Each frame includes a program identifier, PID, of which the DOCSIS data is allocated one: HEX 1FFE. The cable modem searches for the channel with the DOCSIS PID when it is powered up. The channel can be any of the system channels but is typically in the digital channel range above 350MHz.

[34] Once the DOCSIS modem finds its downstream data, the dialog begins negotiations with the head end to determine various parameters of operation such as the upstream channel, the

power of the modem's transmitter, modulation technique, symbol rate, and finally the negotiation into an encrypted communications session using X509 certificates based upon a combination of data permanently installed in the cable modem:

- A serial number
- A cryptographic public key
- An Ethernet MAC address
- The manufacturer's identification

[35] Further system authentication integrates the registration of the modem and customer's account within the billing system. The ability to communicate directly with customers or groups of customers sharing a common problem directly relieves a substantial portion of the support burden from both transport and ISP vendors. It will also improve support quality and customer satisfaction.

[36] For the preferred embodiment, the simplest environment, that of a broadband cable system, is used as an example. In such a cable system over which broadband Internet data is offered, there are two basic types of devices in the invention as shown by Figure 1.

Redirecting device -- a device residing in the neighborhood along with the cable access concentrator. This product is intentionally located at the edge of the network, providing intelligence at the last scalable point in the cable operators' IP network (in closest proximity to the user). The number of redirecting devices will replicate the number of access concentrators within the network, and the device will inter-connect to one of the

access concentrator's Ethernet ports, or in a manner as to have access to user upstream traffic. This device could be located anywhere in the infrastructure where access to user upstream traffic is available, but the closer it is located to the user, the greater the possibility for delivering messages due to upstream service outages. In one embodiement, the insertion of the redirecting device includes web cache control protocol., switching or redirecting mechanisms in an existing ISP router may be utilized. In another example, the redirecting device is insertede in the path of web traffic from the user through an ISP.

Consolidating and managing device -- a device located in the cable operator's NOC (Network Operations Center) providing data services and management control to the deployed redirecting devices. This product will be interconnected to the NOC network, which interconnects all of the NOC servers as well as the Internet portal.

[37] Bulletin Services and the Benefits: The location of the bulletin services equipment can be made optimal for solving the very set of problems described above. When located at each uBR/CMTS(Universal Broadband Router, Cisco's name for its Cable Modem Termination System product line), it can survey the state of the upstream and downstream network and automatically provide high visibility of the status to the customer. It can deliver individual content to specified users or groups with individually tailored policies (frequency, circumstances, pop-up, banner, front, back, etc.). It can target customers issuing packets with signatures of virus-generated communication. And, it can determine upstream problems and assign the trouble to either the transport vendor or the Internet service provider for further action, if required, or simply eliminate the call because of the visibility of the problem and the subsequent reinstitution of operation.

[38] The bulletin services clearly can eliminate service calls. Many "problems" are not problems and can be eliminated, such as providing the customer a pre-announcement of a scheduled maintenance downtime or a clear description of an existing, general Internet problem out of the control of the local system. Problems that are quite deterministic as to which vendor owns the responsibility can often be automatically determined. Unless the entire system is totally "dead," the trouble call can be deflected to the responsible vendor with some helpful information. Customers under the influence of a "virus" can cause the system a lot of trouble without the customer having visible symptoms. Real-time communications with the customer can, often automatically, enlighten that customer to the contamination and possibly issue a required repair procedure which, if ignored, might result in the subscription being temporarily disabled.

[39] Direct communication with the Internet access customer has been used effectively for several years through pop-ups and banners, but these have only been issued from the destination site that was sought by the browsing customer. They have been used for extending the advertising viewing space and time as well as for special information bulletins issued from that destination site.

[40] Direct communication with the customer from the transport vendor or ISP vendor, independent of the destination sought by the customer and without blocking the customer's access to that destination has not been previously developed and, therefore, available. However, the services that directly target real-time bulletins can provide a mechanism that forges a general-purpose facility and provide this capability.

- Virtually all calls due to downtime that had been previously scheduled and announced. That could easily be a sizable portion of the installed base.

- Virtually all calls that can be automatically diagnosed as non-local, upstream Internet congestion whether assigned to a particular provider or general Internet malfunctions. Progress on the problem can be presented in a bulletin.

- Virtually all calls that are due to local infrastructure outages that are upstream of the uBR/CMTS. These problems can be diagnosed and announced automatically or manually to the customer. Progress in repair can be highly visible to the customer who will get better information by viewing the real-time bulletin of the progress than holding on a telephone line.

- Virus preventative cut-offs.

[41] Problems in the first category are clearly stated to the customer as being supported by the carried provider. Calls to will be immediately re-directed to the provider. Trouble in the second category is often associated with a general cable outage and usually results in a call to the cable television repair service first. In such cases, both are re-instituted simultaneously and the appearance of a working TV is the signal for the recovery of the cable modem. Troubles in the third category will result in an "informational" call of short duration.

[42] This brief analysis indicates that bulletin services can eliminate most calls, the longest and most complicated calls, and clearly increase customer satisfaction. The reduction in calls affects both Level-1 call-center personnel as well as Level-3 "last resort", highly trained personnel.

[43] The Bulletin Services can reduce other network personnel overhead:

- The location of the bulletin services device at the uBR/CMTS permits it to check every connection for the signature of a virus-generated "storm" that causes system-wide degradation. It is also in the position to be directed, manually, by network personnel, to inform the customer that a virus infection is causing difficulties on his PC and that remedial action is required. A written bulletin can include step-by-step procedures to remedy the problem saving a rather lengthy telephone dialog.

[44] This capability can be extended to react to a variety of signals of misuse activity of the system by customers either automatically or by simple, manual issuance of an appropriate bulletin.

[45] The network support personnel are the most highly paid and notoriously overworked. Reductions in these areas are clearly highly valuable.

[46] Redirecting Device Environment: Figure 2 shows the redirecting device at the network edge with the cable access concentrator/router and other various network components:

- Platform Specification

- Hardware chassis (e.g., NEBS-compliant or standard rack mount, or stand-alone), with processor, RAM, non-volatile storage. This may be offered as an integral hardware solution running a standard or an embedded operating system, or as a software solution running on a standard PC/UNIX/Mac workstation or other computer system.

- Optional facilities for configuration, troubleshooting, and out-of-band management.

- Interface to the provider infrastructure, e.g., Ethernet, SONET, and the like.

[47] Redirecting Device Software Block Diagram: Figure 3 provides a summary of how the redirecting device navigates through the four critical modules. The HTTP engine accepts connections for pages that may need to be replaced, parses URL, determines replacement strategy, provides replacement pages from the policy database, and proxies to a "real" server on an as-needed basis. The management engine receives and stores policy from the system, provides replacement policy as requested by the HTTP engine, notifies the GRE and IP layers (Generic Routing Encapsulation, as defined by RFC 2784) of address policy (i.e., intercept or not, lifetime and the like), and implements management protocol between redirecting and management devices. The address manager is notified by the GRE and/or IP when a new address is detected, and requests address information between redirecting and management/consolidating devices and will asynchronously send to the policy engine. When GRE is used, such as when WCCP is used to insert the redirecting device into the network, the GRE is implemented for high performance, and examines incoming packets from the Ethernet driver. If there is not any fragmentation and the source address is known and does not require interception, the packet can immediately be transmitted back to the router. This ensures good performance for the most likely cases. If fragmentation does exist, the packet is given to the IP layer for further processing and the completed packet is then given by the IP layer back to the GRE for processing. If the IP address includes a policy that requires further processing, the GRE header is removed and sent back to the IP stack for further processing by the HTTP engine.

Alternatively, functions such as IP defragmentation and delivery of replacement pages can be implemented below the IP stack with improved efficiency.

[48] With specific reference to Figure 3, the following should be noted:

- Software Application Specification --WCCP v1 and v2, unicast and multicast, GRE support, L2 support as it becomes available from Cisco.
    - Cisco-like command line interface.
    - SNMP (Simple Network Management Protocol) support as required.
- Protection from access by consumers, e.g., filters and/or SSH (Secure Shell).
    - Keeps policy list by IP address, as provided by Bulletin Manager
    - For non-intercepting IP addresses, packet is vectored back to router at wire speed
    - For intercepting, box must proxy to real server in order to have access to reverse traffic, or a connection to the real server can be allowed and then later intercepted to avoid having to proxy.
- Traffic modification replaces page, which can provide new content, a redirection to a different page (possibly on another server), or provide a pop-up with the main page fetching the originally-requested content
- Traffic modification based on schedule policy:

- One-shot
- Interval
- Frequency-changing interval
- Acknowledgement from user can modify policy
- Policy loaded by Bulletin Manager

[49] Additional Specifications: The consolidating and management device is located in the NOC and licensed based on number of deployed devices within the operating network:

- Platform Specification
  - Same specifications as redirecting device except:
    - Faster CPU with additional RAM
    - Larger storage facility
- Additional Interfaces similar to other NOC oriented hardware

[50] Software Application Specification

- Protocol between devices should be open and publishable
- Front-end management console allows:
- Defining redirecting devices
- Obtaining status/configuration of redirecting devices
- Defining policy

- Loading web pages to be distributed
- Back-end management:
- Monitoring/upgrading redirecting devices
- Integrates with customer systems, including billing
- Integrates with DHCP or other address management system to cross-reference customer ID with current IP address.

[51] Implementation Approach: Whenever a redirecting device receives a TCP SYN packet, it looks in its table to find the IP address of the source. If the address is not in the table, or is expired, it sends a request to the address management device, along with a unique identifier for any policy that it has cached for that IP address (in the case of an expired entry). Depending on configuration, it could then forward the original packet back to the router, or discard or delay the packet. If the address is unknown, it also creates an entry for the IP address with a short expiration, so that it will not query the consolidating and management device again for a little while.

[52] The address management device then queries the address management database (e.g., DHCP) to obtain the Cable Modem address associated with that IP address, and may also obtain the DHCP lease expiration time. Once the consolidating and management device determines the user associated with the IP address, if a message for that user is desired, then it can send new policy information to the directing device along with a unique identifier for that policy. If the unique policy identifier sent by the redirecting device indicates that the redirecting device already has the correct policy information available, then the consolidating and management

device does not need to re-send it; it can just re-activate it. In addition, the DHCP lease expiration time is sent, even if no message is desired. The redirecting device updates its table so that it will not query the consolidating and management device again concerning that IP address until the DHCP lease expires, or more likely, some fraction of that time, perhaps with a limit.

[53] Systems that utilize alternative address management databases to reconcile subscriber account identification with currently issued IP addresses can be used identically to the DHCP query for Cable Modem address within the consolidating and management device by substituting the alternate account identification for the Cable Modem address and subsequently relaying the respective policy information for that subscriber to the redirecting device upon discovery of the associated IP address.

[54] The loading of the policy from the consolidating and management device to the redirecting device is asynchronous from the above processing, i.e., the redirecting device will simply continue to reflect packets for the IP address until the policy information changes. Likewise, if there is a failure in the communications between the redirecting device and consolidating and management device, including the consolidating and management device itself, then the redirecting device will simply reflect packets back to the router.

[55] In some cases, the consolidating and management device will send policy information to the redirecting device before being queried by the redirecting device. When a redirecting device initializes, it will send a packet to the consolidating and management device indicating that it is starting fresh. If the consolidating and management device knows of policy information that should exist in that redirecting device, it can send it ahead of any requests by users.

[56] In addition, a consolidating and management device must maintain a list of addresses located at each redirecting device, so that if consolidating and management device is loaded with new policy information, it can send that policy immediately, rather than waiting for the address lease to expire.

[57] When a consolidating and management device sends a policy to a redirecting device, it should include the IP address, and, for neighborhood-wide messages, a mask, and the message or modification to be performed for that address. When a redirecting device expires the IP address from its cache, it should also deactivate the policy, but keep the policy available. A single policy may be applied to multiple IP addresses.

[58] When a redirecting device receives a connection for which it wants to send a message, it accepts the connection as if it is the server, so that the HTTP GET message is seen. Then, the URL and HTTP header can be examined as required. If it is then desired to send a replacement message, a redirecting device creates a socket that will appear to be the server and send the replacement page back to the user, as if it is the server. If the page is not to be replaced, the redirecting device will connect to the real server and proxy the data back to the user.

[59] Alternatively, the redirecting device reflects packets back to the router while maintaining state information about the browsing session. Once an HTTP GET message is seen and the URL and HTTL header are examined, if it is desired to send a replacement message, the redirecting device replies directly to the user, as if it is the server, and the redirecting device sends a message to the server, as if it is the client, that terminates the session. If the page is not to be replaced, the redirecting device can simply continue to reflect packets back to the router.

[60] Care must be exercised when sending a replacement or modified page to do so at an appropriate point in the data stream. For example, if a GET is requesting a JPEG image, then it is not possible to substitute an HTML document. Only a GET that is requesting an initial page should be allowed. This can generally be determined by examining the HTTP header.

[61] "Neighborhood" or Localized Implementation: An alternative configuration is shown in Figure 4. In this configuration, the redirecting device may be at the aggregation router level or at the CMTS or neighborhood level. In fact, there is not any limitation to the number of redirecting devices in the network and each level provider, at the ISP level, the router level or the neighborhood level, can include an independent redirecting device.

[62] In a Wi-Fi type system, as shown in Fig. 5, the redirecting device is installed between the provider and a router, either using direct routing or as a NAT (Network Address Translator) gateway. This permits the Wi-Fi provider to communicate with each of the users 1-N on the system at any point in time, while still permitting single subscriber connectivity with the ISP. In this configuration, the specific user can be identified behind the NAT by sending a "null" message from the redirecting device to each user on line via the Wi-Fi, as they actively browse, and setting a cookie and examining the existence of such cookies. The examination then identifies each individual user. The Wi-Fi provider can then direct specific to each user on an individual or a group basis.

[63] In the Wi-Fi application, the NAT is connected to a Wi-Fi network typically adapted for accommodating a plurality of users. In its preferred form the redirecting device is configured to identify each of the plurality of users on the Wi-Fi network. This may be accomplished by directing the redirecting device to send a message to all of the users on the Wi-Fi network with a

request for an automatic response. The redirecting device then identifies each of the users from the automatic response. This will then support the ability to send a selected one of the identified users.